WO0109703

Publication Title:

SYSTEM FOR PROTECTING INFORMATION OVER THE INTERNET

Abstract:

Abstract of WO0109703

A system (10) for protecting information over the Internet (16), or other public network, is provided at a web site addressable by one or more client computer systems (18). Each client computer system connects to the web site to receive a respondent identifier and viewer software. A unique viewer identifier is generated by the viewer software at the client computer system (18) and sent to the web site for registering the viewer identifier with the respondent identifier. The web sit 1473 e has a database (20) and one or more web servers (12, 13, 14, 15) coupled to the database. The database (20) stores registration information including the viewer identifier and associated respondent identifiers for the client computer systems (18), encrypted content information files and keys to decrypt such files, survey invitation information for each of the surveys, and exposure limit information. In response to receiving a survey in accordance with an invitation, the client computer system (18) enables the content viewer to connect to the web site of the content protection system (10) and download a file with the encrypted content information for that survey. The viewer software then sends a request to the content protection system (10) for a key to decrypt the downloaded content information file. The content protection system (10) determines, based on the respondent, viewer and survey identifiers and associated exposure limit information, whether to send a decryption key. If so, a decryption key is sent to the client computer system (18) and the viewer uses the key to decrypt the encrypted content information file, and then opens a viewer window to show the decrypted content information on the display of the computer system (18). During viewing on the computer system (18), the viewer limits access to the window showing the displayed content information which would typically allow the user to access information and enable copying.

Data supplied from the esp@cenet database - Worldwide

------------
Courtesy of http://v3.espacenet.com

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 February 2001 (08.02.2001)

PCT

(10) International Publication Number
WO 01/09703 A1

(51) International Patent Classification⁷: G06F 1/24

(21) International Application Number: PCT/US00/20963

(22) International Filing Date: 1 August 2000 (01.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/146,691 2 August 1999 (02.08.1999) US

(71) Applicant: HARRIS INTERACTIVE, INC. [US/US]; 135 Corporate Woods, Rochester, NY 14623 (US).

(72) Inventors: BAYER, Leonard; 38 Gaslight Lane, Rochester, NY 14610 (US). MATHIAS, Nelson; 5 Brewster Lane, Pittsford, NY 14534 (US). FROST, David; 3 Running Creek Circle, Rochester, NY 14623 (US).

(74) Agent: LUKACHER, Kenneth, J.; South Winton Court, 3136 Winton Road South, Suite 304, Rochester, NY 14623 (US).

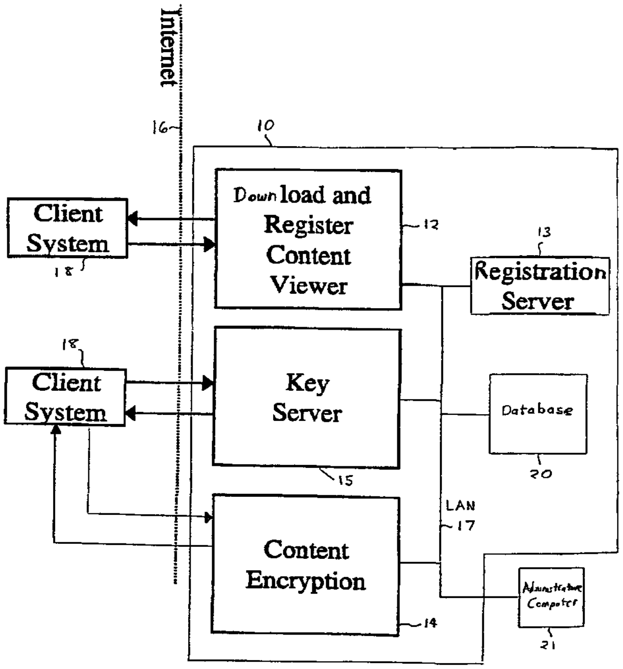
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: SYSTEM FOR PROTECTING INFORMATION OVER THE INTERNET



(57) Abstract: A system (10) for protecting information over the Internet (16), or other public network, is provided at a web site addressable by one or more client computer systems (18). Each client computer system connects to the web site to receive a respondent identifier and viewer software. A unique viewer identifier is generated by the viewer software at the client computer system (18) and sent to the web site for registering the viewer identifier with the respondent identifier. The web site has a database (20) and one or more web servers (12, 13, 14, 15) coupled to the database. The database (20) stores registration information including the viewer identifier and associated respondent identifiers for the client computer systems (18), encrypted content information files and keys to decrypt such files, survey invitation information for each of the surveys, and exposure limit information. In response to receiving a survey in accordance with an invitation, the client computer system (18) enables the content viewer to connect to the web site of the content protection system (10) and download a file with the encrypted content information for that survey. The viewer software then sends a request to the content protection system (10) for a key to decrypt the downloaded content information file. The content protection system (10) determines, based on the respondent, viewer and survey identifiers and associated exposure limit information, whether to send a decryption key. If so, a decryption key is sent to the client computer system (18) and the viewer uses the key to decrypt the encrypted content information file, and then opens a viewer window to show the decrypted content information on the display of the computer system (18). During viewing on the computer system (18), the viewer limits access to the window showing the displayed content information which would typically allow the user to access information and enable copying.

WO 01/09703 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM FOR PROTECTING INFORMATION OVER THE INTERNET

Description

This application claims the benefit of priority to U.S. Provisional Patent Application No. 60/146,691, filed August 2, 1999, which is herein incorporated by reference.

Field of the Invention

The present invention relates to a system (and method) for protecting information over the Internet or other public networks, and relates particularly to, a system for protecting the viewing of information at a computer system which is connected over the Internet to the system. The invention is especially suitable for conducting surveys over the Internet via a computer in which part of the survey viewed on the display of the computer must be protected from unauthorized viewing and copying. The invention may also be applied to any other application where viewing of information at a computer requires authorization and protection from copying, where rights to limited viewing of the information are received via the Internet. Viewing is generally defined herein as displaying graphics, text, video, or other information with any accompanying audio.

Background of the Invention

Conventionally, surveys or polls are a series of questions on a form presented to individuals, called voters, to sample the views of people in a given region or country for political, commercial or entertainment purposes. Surveys are typically conducted either in person, mail, or via telephone to a great number of individual voters. With the development of the Internet and its growing widespread use, surveys can now be taken by persons at their computer. For example, a system for conducting surveys over the Internet are described in U.S. Patent Application 09/243,064, filed February 2, 1999, and International Patent Application No. PCT/US00/02623, filed February 2, 2000. Often surveys are used to test concepts, such as the packaging of a new food product, before companies make an investment in the product or to determine the best way to advertise the product. It is important in concept test surveys that the information used to convey the content of the concept be prevented from view by competitors who could use the information to the disadvantage of the company supporting the survey. This is easy in conventional surveys where the viewed information is provided in a protected environment of in-person polling. However, in surveys conducted over the Internet, the environment of the typical web browser software enables a user easily to copy downloaded information of a survey to a storage file, E-mail, or printer. Thus, it would be desirable to conduct a survey over the Internet in which content information of the survey is protected from unauthorized viewing or copying.

Complicated systems for downloading digital works to computer systems have been developed capable of providing billing and payment to the owners of the digital works based on usage, such as copying or displaying, which may be metered. For example, U.S. Patents Nos. 5,629,980, 5,638,443, and 5,715,403 describe a system for controlling the distribution and use of digital works in which usage rights are permanently attached to each digital work stored in repositories, and rendering systems receiving a digital work have access to the work in accordance with the usage rights attached to the work. In another example, U.S. Patent No. 5,982,891 provides a system for virtual distribution to electronic appliances, such as computers, to enable payment for use, and reporting of use, of content distributed to such electronic appliances. The electronic appliance can have a secure processing unit to provide a processing environment offering tamper resistance. In the electronic appliance, access to distributed content is not allowed unless control information, rules and controls, for that content is present at the appliance specifying usage. These systems, which may use encryption/decryption techniques, are complex in order that they can support traditional commercial distribution and transaction methods for digital works. Unauthorized copying of digital works is primarily prevented by the usage or control information which must be present, or permanently attached, to digital works.

Summary of the Invention

It is the principal feature of the present invention to provide an improved system for protecting information over the Internet from unauthorized viewing and copying.

It is another feature of the present invention to provide an improved system for protecting information over the Internet transmitted to a computer as part of a survey.

A still further feature of the present invention is to provide an improved system for protecting information over the Internet transmitted in a content file to a computer in which no specific usage control information, i.e., information defining how the content file may be used, is provided, or otherwise associated with the transmitted content file, in contrast with prior art distribution systems for digital works.

Yet another feature of the present invention is to provide an improved system for protecting information over the Internet in which a network computer can enable a client computer having received an encrypted content files to be authenticated by the network computer using a plurality of identifiers before the client computer can receive a key to decrypt the content file.

A further feature of the present invention is to provide an improved system for protecting information in which a computer receiving a content file has focus control to protect displayed information from the content file from being readily accessed and thereby copied.

Briefly described, the content protection system embodying the present invention includes a web site addressable by one or more client computer systems for connecting to the content protection system over the Internet or other public network. Each client computer system connects to the web site and receives a respondent identifier and viewer software. When the viewer software is installed at the client computer system, it generates a unique viewer identifier identifying the client computer system. The viewer identifier is sent to the web site for registering the viewer identifier with the respondent identifier. The web site has a database and one or more web servers coupled to the database. The database stores registration information including the viewer identifier and associated respondent identifiers for the client computer systems, encrypted content information files and keys to decrypt such files, survey invitation information for each of the surveys, and exposure limit information to determine whether content information can be viewed by a client computer system. Based on the survey invitation information, if the user of the client computer system has been selected to participate in a survey, the client computer system receives an E-mail invitation to participate including a unique survey identifier associated with the survey and the respondent identifier of the client computer system. The survey may represent any program which requires content information to be viewed in a secure environment. In response to receiving a survey, in accordance with the E-mail invitation, from the web site, or another web site, the client computer system enables the content viewer to connect to the web site of the content protection system and download a file with the encrypted content information for that survey. The downloaded file has no associated information regarding usage of the file by the client computer system. The encrypted content information is identified by a unique content identifier. The encrypted file may alternatively be provided from another source on the client computer system, such as a disk or CDROM. The viewer software sends a request to the content protection system for a key to decrypt the downloaded content information file, and includes in the request the respondent, viewer, survey, and content identifiers. The content protection system determines whether the respondent, viewer and survey identifiers match corresponding identifiers of the participants invited to take the survey stored in the database of the system, determines based on the exposure limit information whether the content information can be viewed at the client computer system, and if the survey has not yet been taken by the user at the client computer system. If so, the decryption key is sent to the client computer system and the viewer uses the key to decrypt the encrypted content information file, and then opens a viewer window to show (graphic or text) or play (video, animation, or audio) the decrypted content information on the display of the computer system. If not, an error message is sent to the client computer system.

During viewing, the viewer ignores interrupts from the keyboard and mouse which typically allow the user to access information and thereby enable copying, such as a print screen key, right mouse button, or screen scraper. If the user selects another window other than the window of the viewer, the viewer stops showing the decrypted content and displays a protection image in its place. Thus, the content information is protected from authorized viewing by encryption and protected from unauthorized copying by limiting the ability of the user access to only viewing.

Brief Description of the Drawings

The foregoing features and advantages of the invention will become more apparent from a reading of the following description in connection with the accompanying drawings in which:

FIG. 1 is a block diagram of the system according to the present invention illustrating the network connection of components of the system with client computer systems;

FIG. 2 is a block diagram of the content protection system of FIG. 1 with a survey server and one of the client computer systems;

FIG. 3 illustrates the tables of the database of the content protection system of FIG. 1;

FIG. 4 is a flow chart showing the encryption by the Content Encryption server of FIG. 1;

FIG. 5 is a flow chart showing the operation for downloading and registering of the viewer software from the content protection system to one of the client computer systems;

FIG. 6 is a block diagram of one of the client computer system of FIGS. 1 and 2 showing the installed viewer software; and

FIG. 7 is a flow chart showing the operation of the system for protecting content information received as part of a survey.

Detailed Description of the Invention

Referring to FIG. 1, the system 10 of the present invention is shown having multiple web servers 12, 13, 14, and 15 at a web site which are capable of establishing a network connection over the Internet 16 or other public network with one or more client computer systems 18. Client computer system 18 represents a desktop, laptop, WebTV, or other computer system having typical web browser software, such as Microsoft Explorer or NetScape Navigator, and network interface, such as a modem, or Tl/T2 data line to an Internet Service Provider, for communicating to web sites at Internet addresses associated with such sites. The web servers 12-15 are connected to a LAN 17 and have access to database 20. The Download and Register Content Viewer server 12 is coupled to the Internet 16 and has an Internet address or URL enabling a user at client computer system 18 to connect to the web server 12 and download a file referred to as content viewer software. The Registration server 13 updates and maintains registration information in the database 20 identifying the client computer system and installed content viewer software at the client computer system. The Content Encryption server 14 provides for assigning a unique identifier to each content file representing information, such as an image, text, video, audio, or animation, encrypting the content file, determining a decryption key for the encrypted content file, and storing the content file at a URL on the server 14 or another web site on the Internet. The server 14 also allows a client computer system 18 to receive an encrypted content file at the URL associated with the file. The Key server 15 has a URL addressable by the viewer software installed at the client computer system 18 to request the decryption key associated with a downloaded encrypted file. The database 20 stores in addition to registration information and information about each encrypted content file, exposure limit information on the rules regarding when the content may be viewed and how many times the content may be viewed at a client computer system, and survey and invitation information defining the survey requiring viewing of content files and the participants (registered client computer systems) selected for each survey, as will be described later in connection to FIG. 3. The database 20 may be stored in memory, such as the hard drive or RAM, of a computer or another server, or may be contained in memory of one of servers 12-15.

One or more administrative computers represented by computer 21 can be coupled to LAN 17. The administrative computer 21 can send content files to the content encryption server 14 for encryption, and update the database with regards to the survey, invitation information and exposure limit information.

Referring to FIG. 2, the content protection system 10 of the present invention operates to enable a user to view encrypted content files which are called as part of a survey received from a survey server 22. A survey represents an HTML file which is downloaded to the client server and viewed via the web browser of the client computer system. Each survey has a unique identifier called a SurveyID. The survey may be addressed in reference to a SurveyID, or the SurveyID may be referred in the downloaded HTML file. The survey represents questions and each question has an answer set having buttons or text entry fields, which simulates a written survey. A submit button at the bottom of the survey page on the screen may be clicked upon by the user, such as via a mouse, to send the selected answers to each question to the survey server 22 for tabulation. The survey may be conducted over the Internet as described in U.S. Patent Application No. 09/243,064, filed February 2, 1999, and International Patent Application No. PCT/US00/02623, filed February 2, 2000, which are herein incorporated by reference. A survey, which requires the user to view a content file encrypted by the content protected system before answering one or more questions, may automatically enable the content viewer, if installed on the client computer system, to connect to the URL of the content protection system's Content Encryption server 14 to first obtain the encrypted content file and then request the decryption key from the Key server 15. The user at a client computer system 18 can receive an invitation, such as in an E-mail message, to link to the address of the survey server, or the user can address the survey server. Although reference is made to a survey, the survey may represent any program or file which requires information to be viewed. Further, the survey server may be a separate web site, or can be included in the web site of the content protection system.

Records of multiple tables are stored in database 20 shown in FIG. 3. The records of the Exposure Limit 25 and ContentView 26 tables store exposure limit information. The records of the Respondent table 30 store registration information. The records of the Survey 27 and Invitation 29 tables store survey and invitation information. The records of the SurveyContent 24 and Content 28 tables store the information regarding the content files. Each table is related to each other by one or more identifiers defined as follows: ContentID is an identifier to an encrypted content file; SurveyID is the identifier of a particular survey; RespondentID is an identifier for an invitation to take a survey or view secure content; ViewerID is an identifier which uniquely identifies a client computer system for an instance of the viewer software downloaded to a client computer system. The RespondentID need not be unique, but when combined with the ViewerID may be considered unique in representing a survey participant.

The SurveyContent table 24 has two data fields, SurveyID and ContentID. Each record in the SurveyContent table links a particular survey having the SurveyID to an encrypted content file having the ContentID. The Exposure Limit Table 25 has records with the following data fields: ContentID; SurveyID; EndDate, the last date which the encrypted file associated with the ContentID of the record can be viewed; EndHour, the time (hour and minute) on the EndDate when the encrypted file associated with the ContentID of the record can no longer be viewed; StartDate, the first date which the encrypted file of the ContentID of the record can be viewed; StartHour, the time (hour and minute) on the StartDate when the encrypted file associated with the ContentID of the record can be viewed; and No Viewing, a number indicating the number of times the encrypted file associated with the ContentID can be viewed by a client computer system. The View Content table 26 has records with the following data fields: ContentID; SurveyID; RespondentID; and Count, the number of times the client computer system associated with the RespondentID has viewed the content file associated with the ContentID for the survey associated with the SurveyID of this record. The Survey table 27 has three data fields: SurveyID; SurveyURL, the network address of the survey at the survey server; and SurveyName, the name of the survey. The Content table 28 has records with the following data fields: ContentID; ContentName, the name of the encrypted content file associated with the ContentID of this record; and Unlocking Key, the decryption key associated with the encrypted content file associated with the ContentID of this record; ContentURL, the network address where the encrypted content file of the ContentID of this record can be accessed. The Invitation Table 29 has records with the following data fields: RespondentID; SurveyID; ViewerID; Survey Complete, the date and time when the survey associated with the SurveyID was completed at the client computer system having the RespondentID and associated ViewerID; and Survey Start, the date and time when the survey associated with the SurveyID was started at the client computer system having the RespondentID for the associated viewer software ViewerID. The Respondent Table 30 has records with the following data fields: RespondentID; ViewerID associated with the RespondentID; and E-mail, the E-mail address of the RespondentID. In the example of tables 25-30 shown in FIG. 3, each of the types of different data fields are indicated by "I" for an integer number, "D" for date, "T" for time, "VA" for variable alphanumeric followed by a number indicating the maximum character length, and "A32", for a fixed length alphanumeric of 32 characters. The database tables 25-30 will further be described in connection with FIGS. 5 and 7.

Referring to FIG. 4, the administrative computer 21 can send unencrypted (clear text) content file to the Content Encryption server 14 with a ContentID and name to be associated with the content file. The content file may contain data in the form of text, graphics, video, or audio, and can represent a commercial or advertisement for a product or service. The Content Encryption server 14 processes the unencrypted content file 32 in accordance with an encryption algorithm 33 to provide an encrypted content file 34, a decryption (unencryption) key 35, and an encrypted ContentID 36. The encryption algorithm 33 may be any type of typical encryption algorithm requiring an unencryption key associated with an encrypted file. For example, the encryption algorithm may be in accordance with the Federal Data Encryption Standard (DES). Server 14 creates a record in the Content table 28 specifying the ContentID, the Content Name, Decryption key, and the URL where the encrypted content file is stored. For a survey, multiple records are provided in the Invitation table 29 for the survey's SurveyID, where each record has a ViewerID associated with a particular client computer system and a RespondantID associated with the ViewerID for that survey. In this manner, the participates are selected for a survey. This selection may be made randomly from the pool of records of the Respondent table 30 by server 14, or the administrative computer may select each of the participants from the records of the Respondent table. The records in Respondent table 30 in addition to E-mail addresses may have data fields storing other information entered at registration, such as age or sex, or other information typically used to select participants in polling.

For each survey (or program) requiring the viewing of one or more encrypted content files, the administrative computer 21 adds a record to the SurveyContent table 24 of the database linking the encrypted content file, ContentID, with the particular survey, SurveyID. Further, a record in the Exposure Limit table 25 is created specifying for the encrypted content file, ContentID, and SurveyID, the number of viewings for each client computer system, the start date and time of the content file may be viewed, and end date and time the content file may be viewed. Further, each survey, SurveyID, may have a record in the Survey table 27 specifying the URL associated with the survey at the survey server 22, and the name of the survey. The URL may be specified by the administrative computer or by the server 14. The administrative computer may be programmed with an administrative interface for updating (adding, deleting, or changing) the records in the tables 25-30 of database 20 in which edit fields correspond to the data fields of the tables.

Before a user can participate in the survey requiring viewing of the information of a content file, the content viewer must be installed on their computer system 18. To receive the content viewer software, the content control system 10 sends from server 12 to the client computer system of a user an E-mail invitation to participate in a survey in the future with the URL of the server 12 (step 38), as shown in FIG. 5. Each E-mail invitation contains a RespondentID. The URL of server 12 enables the web browser of the client computer system 18 to link to a page at server 12 which enables the user to send a request to download of the content viewer software (step 39). This request includes the RespondentID received via the E-mail Invitation. In response to receiving the request, server 12 sends the content viewer program with an installation program (step 40). The client computer system 18 receives the content viewer and installation software, and the installation program of the viewer is manually executed by the user at the client computer system 18 to install the viewer in memory of the computer, such that it can be called when needed by a survey received from the survey server 22 (step 41). The installation program registers the content viewer in the Windows registry of the client computer system with a specific application type so a file with the same extension can invoke the viewer. The registration process generates a unique ViewerID to identify the client computer system 18, such as described below. After installation of the viewer, the E-mail invitation asks the client computer user to register the content viewer with server 12 by browsing to a URL, or via a dialog box which appear at the end of the viewer installation, to complete the registration. By connecting to this URL, the ViewerID is sent to server 12 to be stored (registered) in a record of the Respondent table 30 of the database with the RespondentID received in the E-mail invitation (step 42). The user is also asked during registration for their E-mail address and any other information to be stored in this record.

The ViewerID may be generated by a call to the Win32 system API CoCreateGUID. The ViewerID is generated to uniquely identify the client computer system 18, and may be based on: the current date and time, a clock sequence and related persistent state to deal with retrograde motion of clocks, a forcibly incremented counter to deal with high-frequency allocations, and the truly globally unique IEEE machine identifier, obtained from a network card, or other highly variable machine states. Thus, the registration process now ties together, in Respondent table 30 of database 20, the user's original E-mail address, the RespondentID sent to the user at the start of the registration process, and the ViewerID generated during viewer installation. If the user changes his E-mail address, the user must re-register his copy of the viewer, as described above.

Referring to FIG. 6, the client computer system 18 and installed content viewer software 44 is shown. The client computer system 18 operates on the window operating system or platform, typically referred to as the Win32 environment. The computer 18 has memory (RAM or hard disk drive) storing the encrypted content file 46 downloaded from the web site of the content protection system. Alternatively, the encrypted content file may be stored on a disk or CDROM received via a disk or CDROM drive of the client computer system 18. The content viewer 44 has several modules, and operates using API and DLL functions (or calls to programs) in Win32, as shown in FIG. 6. In the Traffic/Cache Control Module 48, the communication with the content encryption server 14 is conducted using WinInet API calls, as typical of network communication between a web server and a client computer. Once the communication is established, the same set of API calls are used to download encrypted content from the referenced URL's. Further, at module 48, once the content is downloaded, the content is stored in the client computer's cache directory. These files are accessed using the URLCacheAPI. After the content is downloaded and decrypted, the keyboard, mouse and focus control are handled by hooks to the Win32API and the VB6 runtime DLL library. The Decryption Control Module 50 utilizes Window's CryptAPI to call to the viewer from the Window operating system for decrypting the data of encrypted file in accordance with a received decryption key, and Window's AdvAPI call to send the decrypted image to the screen of the display 51 of the client computer system 18. When a decrypted image is displayed on the screen, the Event Control Module 52, via the Win32API, monitors interrupt events 53 from the mouse and keyboard (i.e., user interface). The Focus Control Module 54 is activated if the user switches focus away from the content viewer, such as the Alt-Tab, pressing of the left button on the mouse, clicking on another window on the screen or the screen's desktop. The Focus Control Module 54 in response to a switch in focus from the user, immediately stops the viewer from showing the decrypted content information, and instead shows a protection image in the window of the content viewer, such as a gray screen with a copyright notice or other information.

Referring to FIG. 7, the operation of the system will now be described. The content protection system sends to a client computer system 18 an E-mail invitation to participate in a survey based on the records in the Invitation Table for the SurveyID associated with the survey (step 56). The Key server locates each RespondentID to participate in the survey using the records of the Invitation table associated with the SurveyID of the survey, and then related records in the Respondent Table for E-mail address associated with the RespondentID. The E-mail invitation, in addition to a message requesting their participation in the survey, includes the SurveyID and RespondentID and the URL of the survey server 22 (FIG. 2). Although this invitation is preferably E-mail, the same information may be sent to the user through regular mail or other advertising media. The invitation contains a network address of the survey server which references the SurveyID of the survey. In the case where an E-mail invitation is used, the address may be in an embedded hyperlink upon which the user clicks upon to contact the survey server and receive the HTML page with the survey. The RespondentID may be an embedded as a parameter in the URL, or the opening dialog box of the survey may request it from the user. (The RespondentID may have been given to the user, such as by display to the user, at the earlier described registration process). Upon receipt of the survey, the web browser of the client computer system operates in accordance with the HTML code of the survey to enable the viewer, which then sends a request to the web site of the content protection system for the encrypted files based upon the SurveyID (step 57). In response, the content protection system, such as server 14, queries for all records of the SurveyContent table having the SurveyID and locates the ContentID associated with the SurveyID. In addition, the SurveyStart field of the record of the Invitation table for the RespondentID is updated with the current date and time to show that the survey has commenced. The record of the Content table having the ContentID is then accessed to locate the URL where the encrypted content information file will be found. This URL points to a file which contains the location of the encrypted content. This encrypted content file is then downloaded from this URL address to the client computer system, via the content viewer, at the client computer system (step 58). If multiple records were located in the Content table for the SurveyID, each encrypted content file is separately downloaded to the client computer system immediately prior to processing.

After receiving the downloaded file, the HTML code for the survey (or the content viewer) operates the viewer to send a request, via the Internet, to the Key server 15 (FIG. 1) for the decryption key for the downloaded file (step 59). The request includes the RespondentID and ViewerID which was stored with the viewer when installed, the SurveyID of the survey, and the ContentID of the encrypted content file.

At steps 60-61, the Key server 15 receives, via the Internet 16, the request from the client computer system 18, and sends the decryption key from the record of the Content table 28 having the ContentID to the client computer system requesting the key if the Key server:

1) can locate the RespondentID, SurveyID and ViewerID of the request in the same record of the Invitation table 29;

2) the current date and time is within the specified time period, i.e., date and time range (StartDate, StartHour, and EndDate, EndHour), of the record of the Exposure Limit table 25 for the ContentID and SurveyID of the request;

3) if a record is present in the View Content table 26 having the ContentID, SurveyID, and RespondentID of the request, that the Count field of the record is less than the No Viewing field of the record in the Exposure Limit table 25 for the ContentID and SurveyID of the request; and,

4) the Survey Complete field of the Invitation table 29 having the RespondentID, SurveyID and ViewerID of the request, is not set to a date and time (i.e., indicating that the survey has not yet been taken).

If either conditions 1-4 are not true, an error message is sent to the client computer system 18 from the Key server 15. After sending the key, if a record exists in the View Content table 26 for the ContentID, SurveyID, and RespondentID of the request, the Key server increments the count value by one, otherwise the Key server adds a record in the View Content table for the ContentID, SurveyID, and RespondentID and the count value is set to one. Thus, condition 1 confirms matching of ID's to that of the request to identify preselected invited survey participants, while conditions 2-4 represent examples of business rules to authorize sending of the key. Any number or different business rules may be used, and are not limited to those specified above. For example, although preferably conditions 1-4 must be true, the system may operate using only conditions 1 and 4, if no associated record for the SurveyID are present in the Exposure Limit table or the View Content table, respectively.

The key is received by the viewer of the client computer system, the viewer decrypts in real time the encrypted file, opens a viewer window, and shows (graphic or text) or plays (video, animation, or audio) the decrypted content information on the display screen of the computer system (step 62). The viewer may call a player installed at the client computer system, such as Microsoft Media Player, in accordance with the type of decrypted content information, if needed to utilize the decrypted content information. However, if an error message is received by the client computer system instead of a key, it is also displayed on the display screen.

During viewing, the viewer checks the interrupts received from the keyboard and mouse (or other user interface device of the client computer system) and ignores the interrupts which would enable the user at the client computer potential access to the decrypted content information. If interrupt signals representing the right mouse key, print screen key, or screen scraper are received by the windows operating system, the viewer discards the interrupts. If the window loses focus, such as by the user clicking, via the mouse, on another window on the screen, the viewer window displays only a screen with a copyright notice or other message. Play of display resumes when the viewer again receives focus, such as by the user clicking, via the mouse, on the viewer window.

After viewing is completed, the user can close the viewer window and proceed to answer the questions of the survey. The user submits the answers by clicking on a button on the survey page, which sends the answers to the survey server and a message to the content protection system, i.e., Key server, that the survey was completed with the RespondentID, SurveyID and ViewerID. The survey complete field of the record in the Invitation table 29 having the RespondentID, SurveyID and ViewerID is updated with the date and time the message was received.

Upon receiving a survey invitation, if the client computer system 18 cannot call the content viewer software (since it has not been installed), the HTML code of the survey will not operate. The Key server 15 will allow the installation and registration of the content viewer. However, the client computer system 18 will still not decrypt the content for this particular survey, since there will be no corresponding record in the Invitation table of database 20. Once registered, the client computer system 18 may receive future invitations to participate in surveys with protected content that the user will be able to complete successfully.

In this manner, user interaction with the client computer system 18, via its user interface, is limited during display by the viewer to prevent access to the decrypted content file, and thereby possibly unauthorized electronic copying or printing. As the focus control limits access, no specific usage control information, defining how the content file may be used at the client computer, need be associated or attached with each content file in the client computer system, as in complex prior art distribution systems for digital works. Thus, the content file is not transmitted to the client computer system 18 with usage control information.

The data structures of the tables of the database 20 described above are exemplary. Other data structures may be used with different tables for storing the information described therein.

From the foregoing description, it will be apparent that an improved system for protecting information over the Internet has been provided. Variations and modifications of the herein described system and other applications for the invention will undoubtedly suggest themselves to those skilled in the art. Accordingly, the foregoing description should be taken as illustrative and not in a limiting sense.

Claims

1. A system for protecting information received over a network comprising:

at least one first computer system connected to said network;

a plurality of second computer systems capable of connecting to said first computer system through said network in which each of said second computers has a user interface to enable the user of the second computer to interact with the second computer system;

means for registering at said first computer system one or more of said second computer systems with said first computer system;

means for sending content information from the first computer system to at least one of said registered second computer systems without associated information defining the use of said content information by said second computer systems; and

means for enabling display of the received content information at the registered second computer system which receives the content information and limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information when said received content information is being displayed.

2. The system according to Claim 1 wherein said content information sent to said one of said registered second computer systems is encrypted, further comprising:

means at said second computer system for requesting a key from said first computer system for decrypting said received encrypted content information;

means at said first computer system for sending a key to decrypt the encrypted content information to the second computer system which requested the key; and

means at the second computer system for decrypting the encrypted content information in accordance with the received key, in which said second computer system when displaying the decrypted content information ignores signals from the user interface capable of enabling access to the decrypted content information.

3. The system according to Claim 2 wherein one or more of said registered second computer systems are preselected to view the content information, and said key sending means only sends said key to said preselected second computer systems.

4. The system according to Claim 2 wherein said key sending means only sends said key during a certain time period.

5. The system according to Claim 2 wherein said key sending means only send said key to said second computer system a certain number of times.

6. The system according to Claim 1 wherein said display enabling means at said second computer systems is provided by viewer software installed at the second computer system, and said registering means is enabled when said viewer software is installed.

7. The system according to Claim 1 wherein said sending means, and display enabling means are enabled by viewer software installed at the second computer system.

8. The system according to Claim 7 wherein said viewer software is automatically executed in response to executing a program received by said second computer system via the network.

9. The system according to Claim 1 wherein said second computer systems have a display, and said display enabling means provides for playing said content information is a window on the display.

10. The system according to Claim 9 wherein said display enabling means disables playing of said content information in said window when the user of the second computer system selects another window on the display.

11. The system according to Claim 10 wherein said display enabling means places a protection image in the window when said playing of said content information in said window is disabled.

12. The system according to Claim 1 wherein said first computer system comprises one or more server computers and a database coupled to at least one of said server computers containing at least information defining the registered second computers.

13. The system according to Claim 1 wherein said second computer systems each have means for interfacing to said network and capable of connecting to said first computer system at one or more network addresses.

14. The system according to Claim 1 wherein said network represents a public network.

15. The system according to Claim 1 wherein said content information is part of a survey.

16. The system according to Claim 15 wherein said first computer system comprises one or more server computers capable of communicating with said plurality of second computer systems via said network, and a database coupled to at least one of said network computers containing at least information defining the registered second computer systems, information identifying which of the registered ones of said second computer systems are associated with participants for the survey, and information determining whether the survey was taken by the participants, in which said content information is sent encrypted by said first computer system, said first computer system has means for sending to said second computer systems a key to decrypted the encrypted file when, in accordance with said database, said second computer system is associated with one of the participants for the survey not having taken the survey, and said second computer system has means for decrypting said encrypted content information in accordance with said key for displaying the decrypted content information.

17. A method for protecting information received over a network, such as the Internet, comprising the steps of:

providing at least one first computer system;

providing a plurality of second computer systems capable of connecting to said first computer system through said network in which each of said second computers has a user interface to enable the user of the second computer to interact with the second computer system;

registering at said first computer system one or more of said second computer systems with said first computer system;

sending content information from the first computer system to at least one of said registered second computer systems without associated information defining the use of said content information by said second computer systems; and

displaying of the received content information at the registered second computer system which receives the content information and limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information when said received content information is being displayed.

18. The method according to Claim 17 wherein said content information sent to said one of said registered second computer systems is encrypted, said method further comprising the steps of:

requesting at said second computer system a key from said first computer system for decrypting said received encrypted content information;

sending from said first computer system a key to decrypt the encrypted content information to the second computer system which requested the key; and

decrypting at the second computer system the encrypted content information in accordance with the received key, in which said second computer system when displaying the decrypted content information ignores signals from the user interface capable of enabling access to the decrypted content information.

19. The method according to Claim 18 further comprising the step of selecting one or more of said registered second computer systems to display the content information, and said key sending step only sends said key to the preselected second computer systems which requested the key.

20. A method for conducting a survey at a computer connected to the Internet comprising the steps of:

sending a survey to the computer via the Internet which references a network address to obtain a file for said survey;

downloading said file from said network address in which said file is encrypted;

requesting a key to decrypt said encrypted file from a network address where said key is available;

receiving a key at the computer when said computer is associated with a participant selected to take said survey; and

decrypting the file in accordance with said key and playing the decrypted file as part of the survey.

21. The method according to Claim 20 further comprising the steps of:

playing the decrypted file in a window on a display coupled to the computer; and

protecting said window from being accessed by the user of the computer when another window on the display is selected.

22. The method according to Claim 20 further comprising the step of registering the computer for receiving said survey prior to carrying out said sending survey step.

23. The method according to Claim 20 wherein said receiving a key step further comprises the step of sending the key to the computer when said key has been requested during a certain period of time.

24. The method according to Claim 20 wherein said receiving a key step further comprises the step of sending the key to the computer when computer has not already received the encrypted file a preset number of times.

25. The method according to Claim 20 wherein said receiving a key step further comprises the step of sending the key to the computer when a participant has not taken the survey.

26. A system for protecting an information file received over a public network from a World Wide Web site by one or more computer systems capable of communicating via the network to the web site, said system comprising:

a web site connected to the network which uniquely registers one or more of said computer systems identifying said computer system to said web site and stores in a database encrypted information files and their associated keys, in which said web site is capable of sending said encrypted information file to registered computer systems, and sending a key to decrypt an encrypted information file to one of said registered second computer system when said second computer system is authorized to receive the key;

each of said computer system being capable of connecting to said web site through the Internet and registered with said web site to send a request to said web site for a certain encrypted information file and to receive the encrypted information file, and then request a key from said web site to decrypt the file, and in response to receiving the key, decrypts the encrypted information file and plays the file through a window on the display of the computer system; and each of said computer systems having a display and a user interface in which, when said file is played, signals from the user interface at the second computer system are ignored which enable access to the decrypted file, and when another window is selected than the window displaying the decrypted file, disables the playing of the decrypted file.

27. An Internet web site for supporting concept surveys which are capable of connecting to one or more client computer systems comprising:

one or more computer servers capable of connecting to the Internet in which said client computer system are registered with said web site; and

a database coupled to one or more of said servers which stores encrypted information files representing parts of one or more surveys and their associated keys, in which said web site is capable of sending said encrypted information file to registered client computer systems for carrying out a survey received by said client computer systems, and sending a key to decrypt an encrypted information file to one of said registered second computer system when said second computer system is authorized to receive the key to enable the client computer system to play the information file as part of the survey.

28. A system for protecting over the Internet viewed information received by one of a plurality of computer systems as part of a survey, said system comprising:

a web site connectable to each of the computer system in which said web site has a database storing encrypted content information and keys to decrypt the content information;

means for providing to each of the computer system from the web site a first identifier associated with a viewer;

means for registering each of the computer systems with the web site based on the first identifier provided from the web site and a second identifier uniquely identifying the computer system and storing in said database said first identifier in association with said second identifier;

means for inviting participants to take the survey associated with a unique third identifier in which said participants represent one or more of the registered computer systems;

means for providing to one of the computer system a file containing encrypted content information having a unique fourth identifier;

means at each of the computer system for receiving the survey and receiving the encrypted content information from the web site associated with the survey;

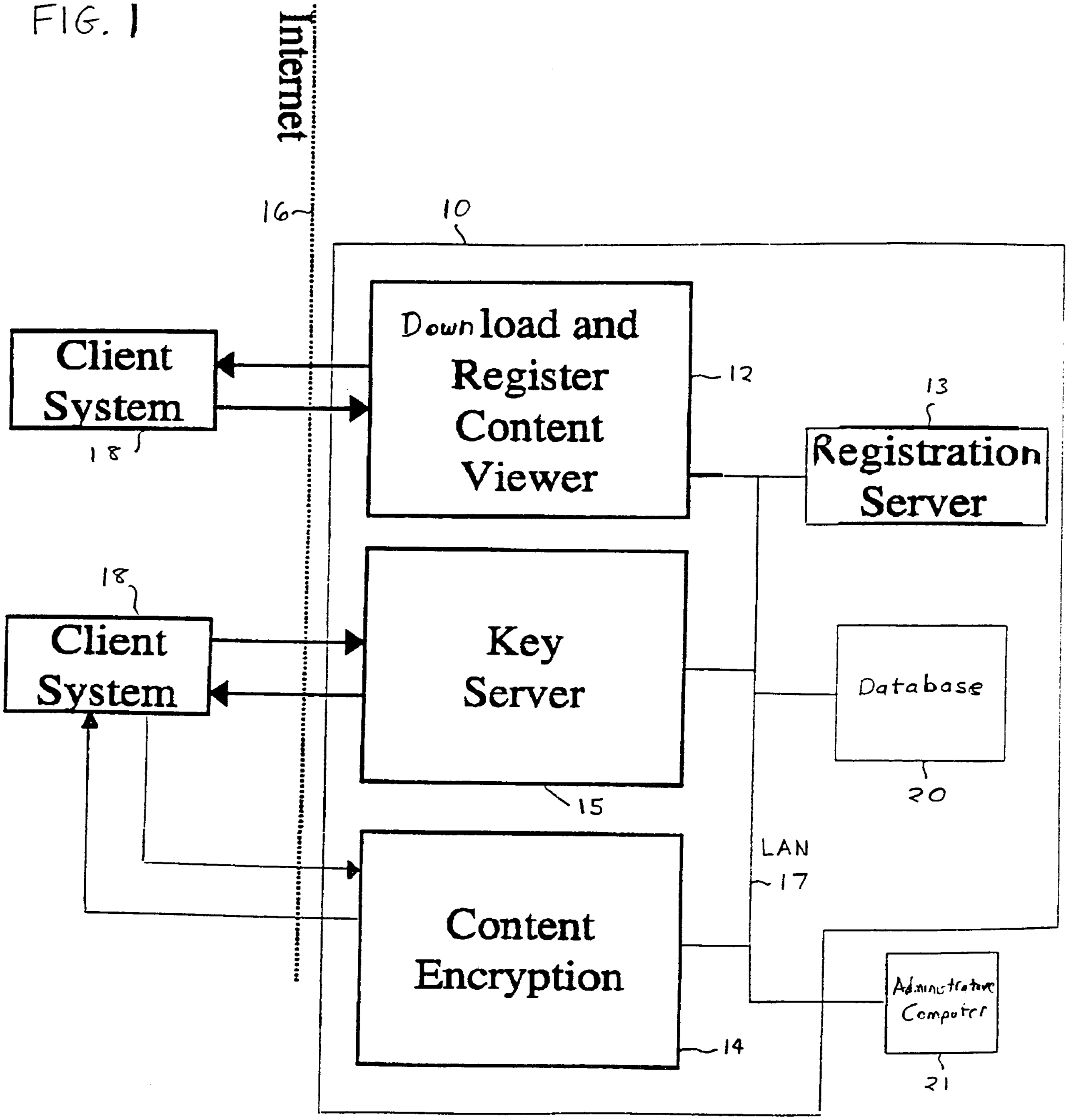
means at each of the computer systems for the viewer at the computer system for sending a request to the web site for a key to decrypt the encrypted content information in which said request has at least said first, second, third, and fourth identifiers;

means for the web site for sending a key to decrypt the encrypted content information file in accordance with the first, second, third, and fourth identifiers of the request matching corresponding identifiers associated with the participants invited to take the survey and exposure limit information associated with the encrypted content information;

means at each of the computer systems including the viewer for receiving the key from the web site, decrypting the encrypted content information based on the key, and opening a window on a display of the computer system to view the decrypted content information file; and

means at each of the computer systems for ignoring interrupts from user interface devices associated with the computer system which enable a user at the computer system to copy the decrypted content information, and for protecting the window when the viewer selects another window on display of the computer system.

FIG. 1


Internet
16
10
Client System
18
Download and Register Content Viewer
12
13
Registration Server
18
Client System
Key Server
15
Database
20
LAN
17
Content Encryption
14
Administrative Computer
21

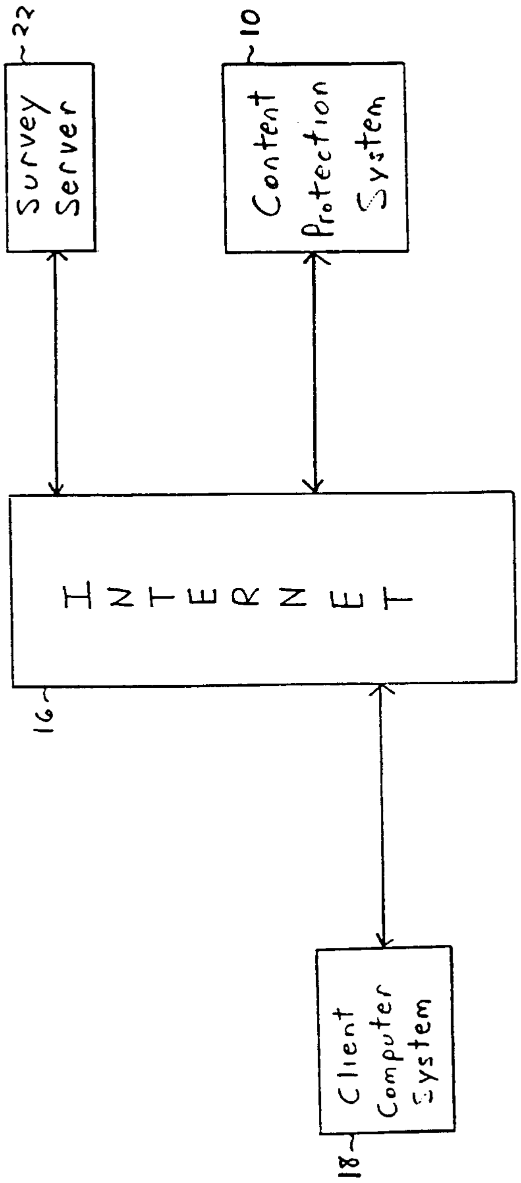

Survey Server
22
Content Protection System
10
INTERNET
16
Client Computer System
18

FIG. 2

FIG. 3

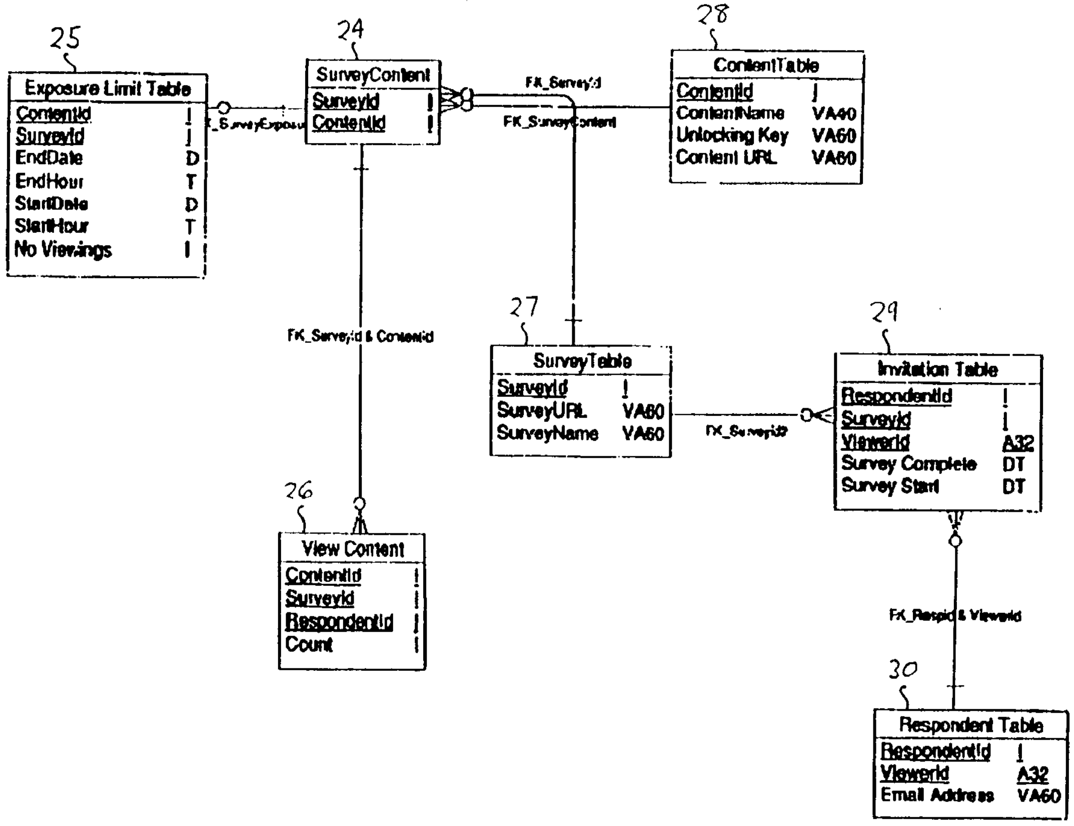

25
Exposure Limit Table
ContentId I
SurveyId I
EndDate D
EndHour T
StartDate D
StartHour T
No Viewings I
FK_SurveyExposu
24
SurveyContent
SurveyId I
ContentId I
FK_SurveyId
FK_SurveyContent
28
ContentTable
ContentId I
ContentName VA40
Unlocking Key VA60
Content URL VA60
FK_SurveyId & ContentId
27
SurveyTable
SurveyId I
SurveyURL VA60
SurveyName VA60
FK_SurveyID
29
Invitation Table
RespondentId I
SurveyId I
ViewerId A32
Survey Complete DT
Survey Start DT
26
View Content
ContentId I
SurveyId I
RespondentId I
Count I
FK_Respid & ViewerId
30
Respondent Table
RespondentId I
ViewerId A32
Email Address VA60

FIG. 4

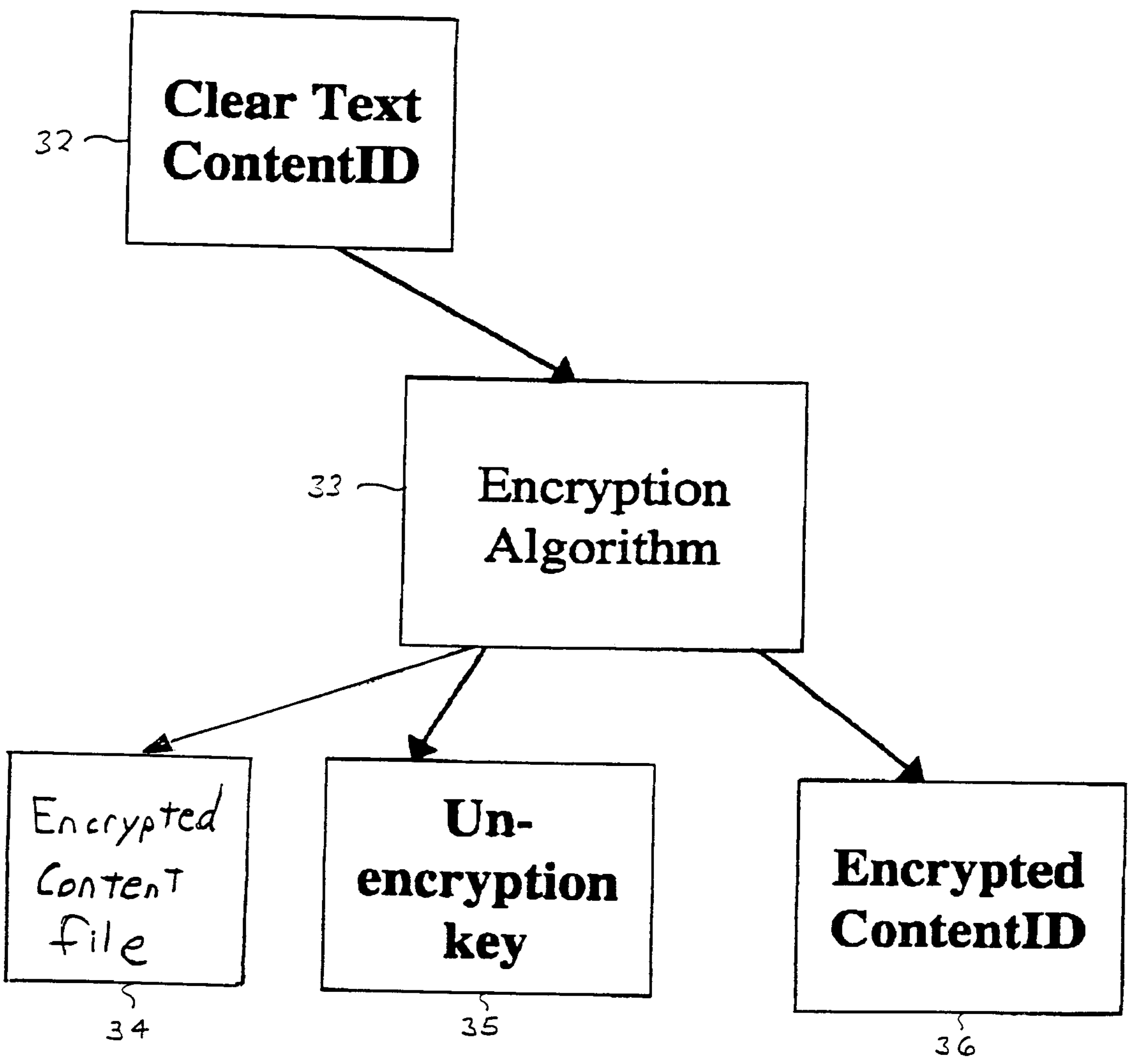
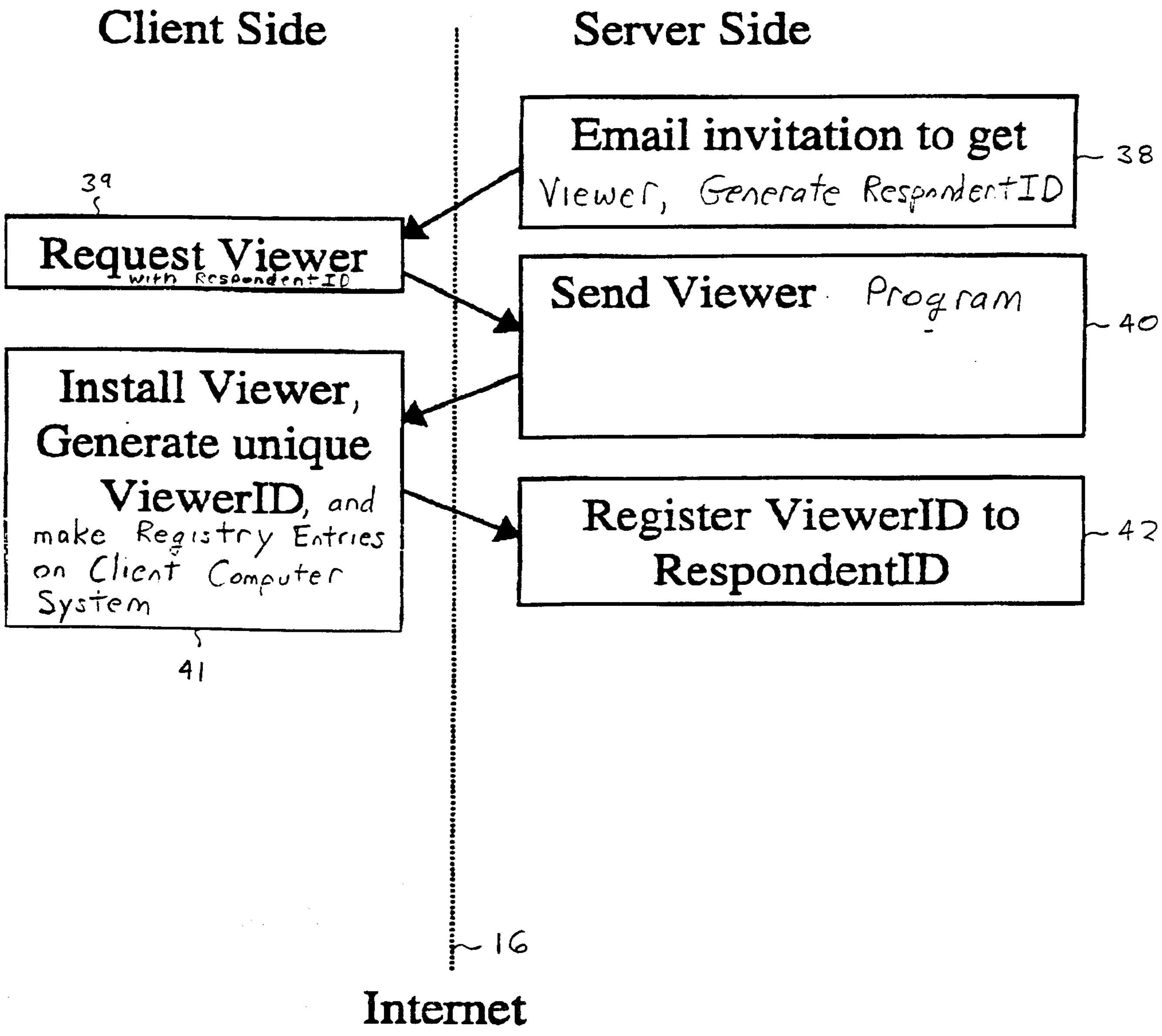

Clear Text ContentID
32
Encryption Algorithm
33
Encrypted Content file
34
Un-encryption key
35
Encrypted ContentID
36

FIG. 5

Download and Register Viewer


Client Side
Server Side
Email invitation to get Viewer, Generate RespondentID
38
39
Request Viewer with RespondentID
Send Viewer Program
40
Install Viewer, Generate unique ViewerID, and make Registry Entries on Client Computer System
41
Register ViewerID to RespondentID
42
16
Internet

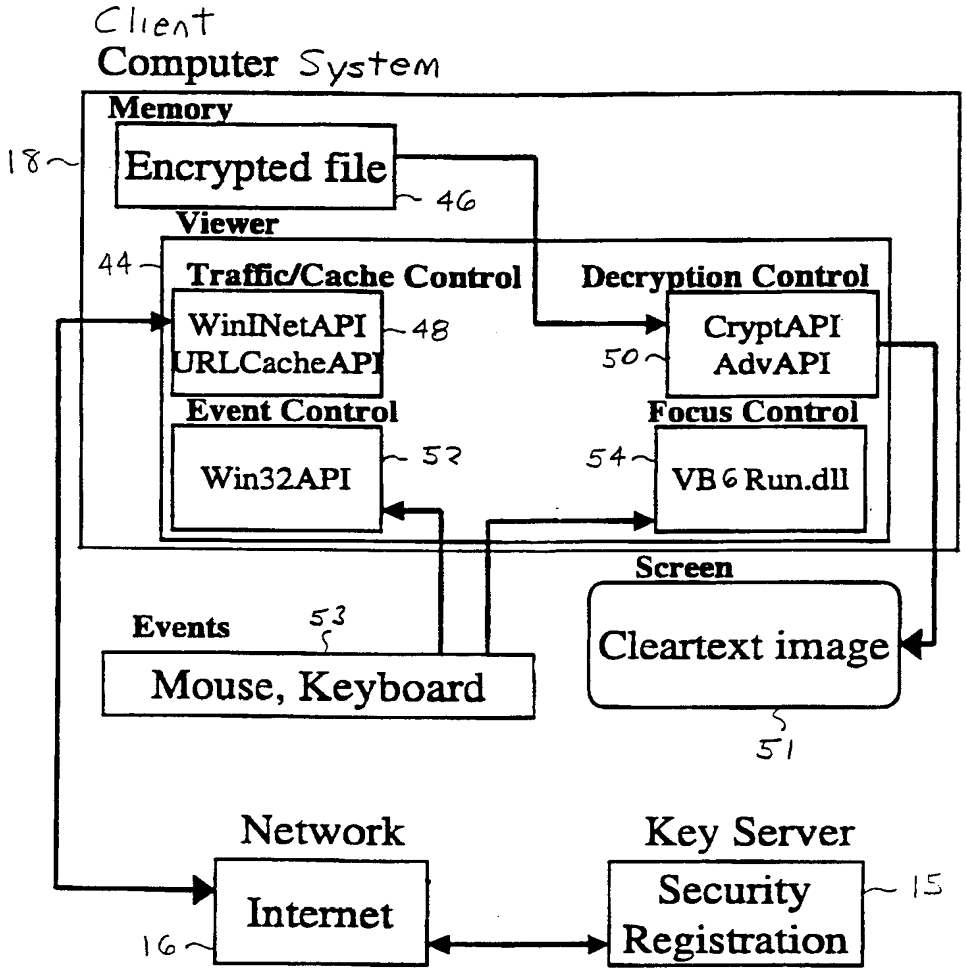
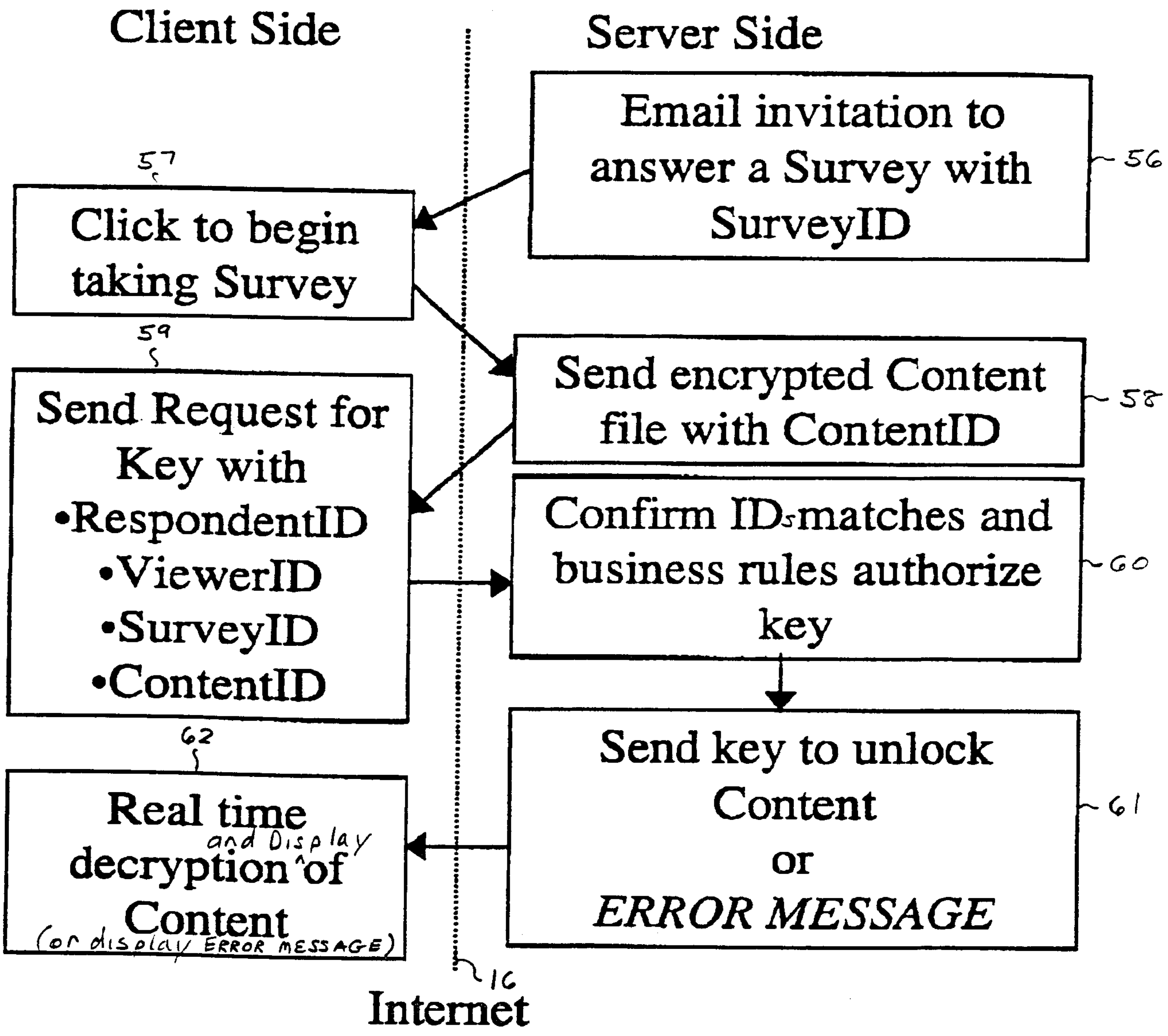

Client
Computer System
Memory
18
Encrypted file
46
Viewer
44
Traffic/Cache Control
WinINetAPI
URLCacheAPI
48
Decryption Control
CryptAPI
AdvAPI
50
Event Control
Win32API
52
Focus Control
54
VB 6 Run.dll
Screen
Cleartext image
51
Events
53
Mouse, Keyboard
Network
Internet
16
Key Server
Security
Registration
15

FIG. 6

FIG. 7

Survey Participation


Client Side
Server Side
Email invitation to answer a Survey with SurveyID
56
57
Click to begin taking Survey
Send encrypted Content file with ContentID
58
59
Send Request for Key with
•RespondentID
•ViewerID
•SurveyID
•ContentID
Confirm IDs matches and business rules authorize key
60
62
Real time decryption and Display of Content (or display ERROR MESSAGE)
Send key to unlock Content or *ERROR MESSAGE*
61
16
Internet

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/20963

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 01/24
US CL :380/255, 277, 281, 28, 30; 713/171, 182, 184
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/255, 277, 281, 28, 30; 713/171, 182, 184

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

West

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,134,661 A (TOPP) 17 OCTOBER 2000, col. 4, lines 14-22, col. 4, lines 37-47, col. 5, lines 1-12.	1-28

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 OCTOBER 2000

Date of mailing of the international search report

14 NOV 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
Peggy Harrod
THOMAS PEESO
Telephone No. (703) 305-9784